Please amend the claims to read as indicated in the following list of claims:

Claims 1- 33. Cancelled.

34. [Currently amended] A method of generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority; the method comprising using computer equipment to apply ~~wherein~~ a bilinear mapping function ~~is used~~ to process multiple data sets each comprising data related to ~~a respective association of trusted authority and~~ the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other.

35. [Currently amended] A method according to claim 34, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on ~~a~~ the secret of the latter.

36. [Currently amended] A method according to claim 34, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and ~~a~~ the secret of the trusted authority.

37. [Currently amended] A method according to claim 34, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key derived from said user identity and ~~a~~ the secret of the trusted authority.

38. [Currently amended] A method according to claim 34, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on ~~a~~ the secret of the latter.

Claims 39 - 42. Cancelled

43. [Currently amended] A computer program product arranged, when installed in computing apparatus, to condition the apparatus for generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority, the conditioned apparatus ~~by~~ using a bilinear mapping function to process multiple data sets each comprising data related to ~~a respective association of trusted authority and~~ the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other; data from the multiple data sets being combined either before or after processing by the bilinear mapping function.

44. [Original] A method according to claim 35, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \leq i \leq n} p\,(R_{\mathrm{TA}i},\, r\, Q_{\mathrm{ID}i})$$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the ith data set,

$R_{\mathrm{TA}i}$ is the public key element of the trusted authority associated with the ith data set, and

r is a random number.

45. [Original] A method according to claim 36, wherein there are n data sets and the decryption key is generated as:

$$p\,(U, \sum_{1 \leq i \leq n} S_i)$$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the ith data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the ith data set.

46. [Original] A method according to claim 37, wherein there are n data sets and the signature key is generated as:

$$p\,(\Sigma_{(1 \leq i \leq n)}\, d_{\mathrm{IDi}},\, P)$$

where:

$p()$ is said bilinear mapping function,

d_{IDi} is the identity-based private key associated with the i^{th} data set, and

P is a public key element of the trusted authority associated with the i^{th} data set.

47. [Original] A method according to claim 38, wherein there are n data sets and the verification key is generated as:

$$\Pi_{(1 \leq i \leq n)} p\,(Q_{IDi}, P_{pubi})$$

where:

$p()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the i^{th} data set, and

P_{pubi} is the public key element of the trusted authority associated with the i^{th} data set.

48. [Currently Amended] A method according to claim 34, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with ~~a~~ the secret of the trusted authority, a public key of the trusted authority.

49. [Original] A method according to claim 34, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

50. [New] A method according to claim 34, wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

51. [New] A method according to claim 34, wherein data from the multiple data sets are combined after processing by the bilinear mapping function.

52. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key concerning a user with which multiple independent user identities are associated, each user identity being intended for use by a respective trusted authority, the computer apparatus using a bilinear mapping function to process multiple data sets each comprising data related to the user's identity with a respective one of the trusted authorities and data related to a secret held by that trusted authority, the secrets of the trusted authorities being unrelated to each other.

53. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

54. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

55. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

56. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

57. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 53, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \leq i \leq n} p\,(R_{\mathrm{TA}i},\, r\, Q_{\mathrm{ID}i})$$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the i^{th} data set,

$R_{\mathrm{TA}i}$ is the public key element of the trusted authority associated with the i^{th} data set, and

r is a random number.

58. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 54, wherein there are n data sets and the decryption key is generated as:

$p\,(U, \sum_{1 \le i \le n} S_i)$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the i^{th} data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the i^{th} data set.

59. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 55, wherein there are n data sets and the signature key is generated as:

$p\,(\Sigma_{(1 \le i \le n)} d_{\mathrm{ID}i}, P)$

where:

$p()$ is said bilinear mapping function,

$d_{\mathrm{ID}i}$ is the identity-based private key associated with the i^{th} data set, and

P is a public key element of the trusted authority associated with the i^{th} data set.

60. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 56, wherein there are n data sets and the verification key is generated as:

$$\Pi_{(1 \leq i \leq n)} p\,(Q_{\mathrm{IDi}}, P_{pubi})$$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the i^{th} data set, and

$P_{\mathrm{pub}i}$ is the public key element of the trusted authority associated with the i^{th} data set.

61. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to claim 52, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with the secret of the trusted authority, a public key of the trusted authority.

62. [New] A computer apparatus for generating an identifier-based asymmetric cryptographic key according to

claim 52, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

63. [New] The computer apparatus of claim 52 wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

64. [New] The computer apparatus of claim 52 wherein data from the multiple data sets are combined after processing by the bilinear mapping function.

65. [New] A computer program product as for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

66. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and the secret of the trusted authority.

67. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key

derived from said user identity and the secret of the trusted authority.

68. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on the secret of the latter.

69. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 65, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \leq i \leq n} p\,(R_{TAi}, r\,Q_{IDi})$$

where:

$p()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the ith data set,

R_{TAi} is the public key element of the trusted authority associated with the ith data set, and

r is a random number.

70. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 66, wherein there are n data sets and the decryption key is generated as:

$$p\,(U, \textstyle\sum_{1 \leq i \leq n} S_i)$$

where:

$p()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the i^{th} data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the i^{th} data set.

71. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 67, wherein there are n data sets and the signature key is generated as:

$p\,(\Sigma_{(1 \le i \le n)}\, d_{\mathrm{ID}i}, P)$

where:

$p()$ is said bilinear mapping function,

$d_{\mathrm{ID}i}$ is the identity-based private key associated with the i^{th} data set, and

P is a public key element of the trusted authority associated with the i^{th} data set.

72. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 68, wherein there are n data sets and the verification key is generated as:

$\Pi_{(1 \le i \le n)}\, p\,(Q_{\mathrm{ID}i}, P_{pubi})$

where:

$p()$ is said bilinear mapping function,

$Q_{\mathrm{ID}i}$ is the identity-based public key associated with the i^{th} data set, and

$P_{\mathrm{pub}i}$ is the public key element of the trusted authority associated with the i^{th} data set.

73. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein:

the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;

the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and

the point associated with the trusted authority forms, together with a combination of this point with the secret of the trusted authority, a public key of the trusted authority.

74. [New] A computer program product for generating an identifier-based asymmetric cryptographic key according to claim 43, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.

75. [New] The computer program product of claim 43 wherein data from the multiple data sets are combined before processing by the bilinear mapping function.

76. [New] The computer program product of claim 43 wherein data from the multiple data sets are combined after processing by the bilinear mapping function.